IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

FAIR FIGHT ACTION, INC, *et al.*,

Plaintiffs,

v.

BRAD RAFFENSPERGER, *et al.*,

Defendants.

Civ. Act. No. 18-cv-5391 (SCJ)

PLAINTIFFS' RESPONSE IN OPPOSITION TO DEFENDANTS' MOTION TO EXCLUDE THE EXPERT TESTIMONY OF J. ALEX HALDERMAN

Table of Contents

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules

Other Authorities

INTRODUCTION

Nearly half of the public has concerns about the security of American elections.[1] Despite widespread concern about the integrity of voting systems, Defendants continue to use election technology that is vulnerable to hacking and manipulation. Technology is significant to Plaintiffs' case. When technology fails, or election officials refuse to take hacking seriously, voters lack confidence their votes will be properly recorded and counted; as a result, some will not vote.[2] Defendants' failure to provide an election system that voters believe is fair to all—regardless of party affiliation, economic power, or skin color—is voter suppression. Faced with reports in 2018 of an insecure system, Defendants reacted by lashing out at critics rather than investigating and remedying the system.

---

[1] *Election Security*, Pew Research Center, available at https://www.pewresearch.org/politics/2018/10/29/election-security/ (last visited July 17, 2020).

[2] Voting technology impacts more than confidence in the system. For example, the existence of long lines may result from an inadequate number of machines, poll pads that do not sync, ballot marking devices that are not working, scanners that will not read ballots, or a failure to train poll workers on the technology. Further, Georgia's chronic technology failures are relevant to the intent to suppress votes because, in choosing to use or misuse out-dated or unreliable technology, the SOS is imposing an unjustified burden on the right to vote.

Plaintiffs' expert, Dr. J. Alex Halderman, has shown that the voter registration system, the 2018 DRE voting machines, and the new Ballot Marking Devices ("BMDs") with accompanying iPads are not secure. Dr. Halderman conducted a rigorous review of Georgia's voting technology and based his report on sound logic and methodology. Dr. Halderman's testimony will aid the factfinder in determining whether Georgia's voting systems are insecure and unreliable, failures that undermine confidence in the validity of the election system and, thus, impose severe burdens on Georgians' right to vote.

Dr. Halderman's opinions are both reliable and relevant, and this Court should deny Defendants' motion to exclude.

STATEMENT OF FACTS

A. Georgia has a history of exposing private voter information.

In 2015, Georgia's voter rolls were breached when the Secretary of State inadvertently disclosed the Social Security numbers and other personal information of six million voters. Kristina Torres, *As many as 7.5 million voter records involved in Georgia data breach*, Atlanta Journal Constitution, Mar. 3, 2017, https://www.ajc.com/news/state--regional-govt--politics/many-million-voter-records-involved-georgia-data-breach/rU2bMMc3tzGkuPvmbjlkgJ/). The year before the 2018 mid-term elections, 7.5 million Georgia voter records were

compromised when the Center for Elections Systems at Kennesaw State University— at the time responsible for oversight of Georgia's election operations and voting machines—allowed a breach of its system. *Id*.

Meanwhile, investigations into the 2016 presidential election disclosed that Russian officers targeted elections. Robert S. Mueller, III, U.S. Dep't of Justice, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, p. 50 (2019), https://www.justice.gov/storage/report.pdf ("Mueller Report"). Russian targets included federal, state, and local entities "such as state boards of elections (SBOEs), secretaries of state, and county governments." *Id*. Additionally, Russia targeted "private technology firms responsible for manufacturing and administering election-related software and hardware." *Id*.

The United States Senate Select Committee on Intelligence ("the Senate Intelligence Committee") also revealed Russian efforts to breach election infrastructure. The Senate Intelligence Committee reported that "Russian activities demand renewed attention to vulnerabilities in U.S. voting infrastructure." Senate Intelligence Committee, *Russian Active Measures Campaigns & Interference in the 2016 U.S. Election*, S. Rep. No. 116-XX, at 4 (2019), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf ("Senate Report"). The Senate Report cited Dr. Halderman's written statement

and testimony when highlighting potential vulnerabilities in U.S. voting machines. *Id*. at 40-42.

The Senate Report further explained that during the 2016 election, "cybersecurity for electoral infrastructure at the state and local level was sorely lacking; for example, voter registration databases were not as secure as they could have been."[3] *Id*. Moreover, "[a]ging voting equipment, particularly voting machines that had no paper record of votes, were vulnerable to exploitation by a committed adversary." *Id*. Threats from Russian hackers are ongoing; the media recently reported that the same Russian groups that targeted the 2016 presidential election continue to target American organizations through malware and other means.[4]

Despite data breaches in Georgia, research showing that electronic voting machines are vulnerable to hacking, and evidence of Russian hacking efforts, Georgia continued to use voter registration data and voting machines that lacked

[3] Defendants were well aware of the systems' vulnerability. One of the cases before the State Election Board involved a county that linked the voter registration system to a computer connected to the internet. (Ex. 1, St. Elec. Bd. Minutes, June 28, 2016 at 195-202 (Case No. 2015-040, Appling County).)

[4] Julian E. Barnes, *Russian Hackers Trying to Steal Coronavirus Vaccine Research, Intelligence Agencies Say*, The New York Times July 16, 2020, https://www.nytimes.com/2020/07/16/us/politics/vaccine-hacking-russia.html

adequate data security for the 2018 election. (Am. Compl. ¶ 94-101, ECF No. 41 at 41-43.) Many Georgia voters were either denied the right to vote—or had their right so impaired as to amount to suppression—in 2018 because of inaccuracies newly introduced into the voter registration system.

Delaney Powers' experience illustrates these inaccuracies. (*See* Ex. 2 (Powers Decl., November 9, 2018).) Prior to the 2018 general election, Ms. Powers verified her address and polling location; on election day, however, state records listed her address incorrectly and she was told that she had to vote at a different location. (*Id.*) The listed address was one at which she had never lived. (*Id.*) Ms. Powers is a disabled veteran with a service dog. She, her husband, their son, and the tired service dog had to go to another part of the county so Ms. Powers could vote. In another example, Eunice Walden was prevented from voting in the 2018 general election. (*See* Ex. 3 (Walden Decl., November 15, 2018).) After voting in DeKalb County for three consecutive years, Ms. Walden was told she could not vote at her polling location because her voter verification notice had been sent to her former address in Macon, Georgia—a location where she had not lived for three years. (*Id.*) She was unable to get to Macon on election day and therefore lost her right to vote. (*Id.*)

During the 2018 election, Georgia also continued to use its DRE voting machines, an electronic voting system that does not create an auditable paper trail for votes. (ECF No. 41 ¶ 94.) Claudine Kelsey described voting on the DRE voting machines and explained how it automatically changed her vote to a candidate that she did not choose. (*See* Ex. 4 (Kelsey Decl., November 19, 2018).) After entering her selection for a third time, the machine finally selected the candidate for whom she wanted to vote; however, she remains unsure if her selection was recorded properly. (*Id*.)

Plaintiffs, organizations that promote voting in Georgia, have complained about security issues. In the Amended Complaint, Plaintiffs challenged many methods of voter suppression that Defendants implement and perpetuate. (ECF No. 41 ¶¶ 68-157.) One mode of suppression is Defendants' use of election technology vulnerable to hacking and manipulation. (ECF No. 41 ¶¶ 94-101.) Vulnerable technology undermines confidence in the election system and causes concerns about "the integrity of the machines." (Ex. 5 (Warnock Dep. 105:1-2).)

The Secretary of State refuses to acknowledge the systems' obvious vulnerabilities, reinforcing that something is amiss. When the U.S. Department of Homeland Security offered security assistance to Georgia, the Secretary of State arrogantly denied that he needed help. (Ex. 6 (Germany Dep. 181:1-183:21).)

When his refusal became public, a voter could not help but conclude that the system was broken or had been rigged. These technical vulnerabilities and the Secretary of State's public refusal to address the issue constitute voter suppression. (Ex. 5 (Warnock Dep. 104:20-105:25).)

After the 2018 election, Georgia passed H.B. 316, which authorized the purchase of new electronic voting machines that would provide "paper ballots which are marked with an elector's choice in a format readable by the elector." *See* O.C.G.A. § 21-2-300(a)(2).

Although Defendants attempted to employ new voting machines for the 2020 Georgia primary election in June, "a cascade of problems caused block-long lines across Georgia, as primary voters stood for hours while poll workers waited for equipment to be delivered or struggled to activate the system's components." Nick Corasaniti et al, *Georgia Havoc Raises New Doubts on Pricey Voting Machines*, The New York Times, June 11, 2020, https://www.nytimes.com/2020/06/11/us/politics/georgia-voting-machines.html. As the media reported, "new machines required too much extra power for aging polling locations, blowing fuses and never powering on [and] . . . workers who were still being trained just days before the election struggled with setup. Some polling places never even received the machines until the morning of the election."

(*Id.*) In her declaration, Ms. Martha Pearson details problems experienced by voters of color at several polls, in particular the fiasco at Christian City where voters waited for four hours and some left without voting. (Ex. 7 (Pearson Decl., June 26, 2020).)

B. Defendants do not question Dr. Halderman's qualifications.

Dr. Halderman's qualifications are not at issue in light of his trio of Princeton degrees, including his Ph.D.; his publications; his teaching responsibilities; his congressional testimony; and his receipt last year of a Carnegie Fellowship for his scholarship in election security. (*See* ECF No. 239 at 45-68.)

C. Dr. Halderman's expert report details the failures in Georgia's systems.

On February 18, 2020, Dr. Halderman submitted his expert report addressing the vulnerabilities of the DRE voting machines used for the 2018 election, the voter registration system, and the new voting machines from Dominion Voting Systems, Inc. (Dominion) currently being implemented in Georgia. (ECF No. 239 ¶¶ 14, 88.) Citing a National Academies of Sciences, Engineering, and Medicine study, Dr. Halderman explained there "is a broad scientific consensus that paperless DREs do not provide adequate security against cyberattacks." (ECF No. 239 ¶ 88.) After considering this study, research, and testing of DREs, Dr. Halderman opined that "Georgia's paperless DRE system was highly susceptible to

cyberattacks that could change votes, erase votes, or cast extra votes." (ECF No. 239 ¶ 88.)

For the Dominion voting machines, which are BMDs, Plaintiffs received documentation from Dominion in response to a subpoena. (ECF No. 239 ¶ 15.) Dr. Halderman reviewed this material, which included technical documentation about the election system components, the company's response to Georgia's Request for Proposals for the new voting system, third-party testing reports, and certain internal engineering memos relating to the security of the system. (ECF No. 239 ¶ 15.) Following this review, Dr. Halderman stated that "Georgia's new voting technology does not achieve the level of security necessary to withstand an attack by a sophisticated adversary such as a hostile foreign government." (ECF No. 239, ¶ 23.)

Dr. Halderman explained how attackers could introduce malware into the election equipment, (ECF No. 239 ¶ 24), described how Dominion software utilizes a "wide range of outdated off-the-shelf software modules," (ECF No. 239 ¶ 30), compared a source code review project for election systems in California, (ECF No. 239 ¶ 29), and noted that Dominion's Chief Security Officer position remains vacant. (ECF No. 239 ¶ 32.) Dr. Halderman's report explained that Georgia certified the Dominion systems without performing its own security test or

source code review. (ECF No. 239 ¶ 33.) Additionally, Dr. Halderman analyzed the voter registration components, electronic poll books, and supply chain threats for the Dominion system and concluded attackers could "infiltrate the voter registration database and extract, change, or erase voter registration records. These attacks could cause voters to receive the wrong ballot or be prevented from casting a regular ballot. (ECF No. 239 ¶¶ 23, 41-51.)[5]

LEGAL STANDARD

Federal Rule of Evidence 702 governs the admissibility of expert evidence related to scientific, technical, or other specialized knowledge. A court may qualify a witness as an "expert by knowledge, skill, experience, training, or education," and the witness may testify in "the form of an opinion or otherwise." Fed. R. Evid. 702.

The trial court is the primary gatekeeper and must determine that the testimony is "sufficiently tied to the facts of the case that it will aid the jury in resolving a factual dispute." *Daubert v. Merrell Dow Pharm.*, 509 U.S. 579, 591 (1993) (quoting *United States v. Downing*, 753 F.2d 1224, 1242 (3d Cir. 1985)).

[5] Dr. Halderman has experimented and published peer-reviewed research specifically about the security of BMDs that informed his opinion. (ECF No. 239 ¶ 54.)

The trial court is also responsible for making "certain that an expert . . . employs in the courtroom the same level of intellectual rigor that characterizes the practice of an expert in the relevant field." *Kumho Tire Co., Ltd. v. Carmichael*, 526 U.S. 137, 152 (1999).

To determine the admissibility of expert testimony, courts apply a three-part inquiry. *City of Tuscaloosa v. Harcros Chems., Inc.*, 158 F.3d 548, 562 (11th Cir. 1998). First, the expert must be qualified to testify on the matter addressed. *Id.* Second, the expert's conclusions must be supported by reliable methodologies. *Id.* Third, the expert's scientific, technical, or specialized knowledge must assist the trier of fact through applying scientific, technical, or specialized expertise. *Id.*

The trial court's role for determining admissibility of expert evidence is critical, but it is not intended to replace the adversary system. *Coshap, LLC v. Ark Corp. Member Ltd.*, No. 1:16-CV-0904-SCJ, 2017 WL 9287017, at *2 (N.D. Ga. Dec. 12, 2017). Generally, "vigorous cross-examination, presentation of contrary evidence, and careful instruction on the burden of proof are the traditional and appropriate means of attacking shaky but admissible evidence." *Daubert*, 509 U.S. at 596. The admissibility of expert testimony, subject to the traditional safeguards of trial, is the general rule, and exclusion is the exception. *See United States v. Brown*, 415 F.3d 1257, 1267 (11th Cir. 2005) ("The question, then, is whether

expert opinion evidence that does not meet three of the four *Daubert* factors nevertheless can be admitted. In the right circumstances, the answer to that question is 'yes.'").

Here, Dr. Halderman has satisfied all the criteria for the Court to admit and consider his testimony. Defendants' arguments are inappropriate for a *Daubert* motion and inform only the weight the Court should assign the evidence, not its admissibility.

ARGUMENT

This Court should admit Dr. Halderman's testimony. First, Dr. Halderman is qualified to testify as an expert regarding cybersecurity of electronic voting systems. Second, Dr. Halderman developed his opinions using reliable principles and methods. In his report, Dr. Halderman offers opinions about the DRE voting system, the BMDs currently being implemented in Georgia, and voter registration components such as the eNet voter registration database. (ECF No. 239 ¶¶ 14-16; 88-101.) Third, Dr. Halderman's testimony is relevant and will assist the Court[6] in determining whether Defendants' vulnerable voting technology and the Secretary

[6] Plaintiffs have filed an Unopposed Motion to Strike the Jury Demand. (ECF No. 465.)

of State's actions lead voters of color to question whether their votes will be counted. (*See* ECF No. 41 ¶¶ 94-101.) His testimony is admissible.

A. Dr. Halderman is qualified to testify regarding cybersecurity.

Defendants concede that Dr. Halderman is qualified to testify regarding cybersecurity of electronic voting systems. (Defs.' Mot. To Exclude Testimony of J. Alex Halderman & Supporting Br. 6, ECF No. 401.)

B. The methodology Dr. Halderman used in his report is reliable.

Defendants question whether Dr. Halderman's report is reliable—whether it is based on sufficient facts and data. *See* Fed. R. Evid. 702(b) (providing a witness may testify if "the testimony is based on sufficient facts or data"). "The reliability inquiry focuses on the principles and methodology underlying the expert's opinion, and not the expert's conclusions." *Coshap*, 2017 WL 9287017 at *2 (citing *Daubert*, 509 U.S. at 595).

Daubert instructs the court to focus on four factors related to the expert's theory or technique. 509 U.S. at 594. These factors include: (1) whether the theory can be (and has been) tested; (2) whether it has been subjected to peer review; (3) what the known or potential rate of error is, and whether standards controlling its operation exist; and (4) whether it is generally accepted in the field. *Id*. at 593-94.

The analysis of these factors should be flexible, rather than rigidly applied. *Id*. at 594 ("[t]he inquiry envisioned by Rule 702 is. . . a flexible one").

Dr. Halderman described the design and architecture for the voting machines, past[7] and present, considering the individual components, how they interacted with each other, and the various controls. (ECF No. 239 ¶¶ 14-19, 88-101.) Dr. Halderman also reviewed Dominion's design and architecture documents and documents from studies related to the 2018 DRE voting machines. (ECF No. 239 ¶¶ 14-19.)

Next, Dr. Halderman summarized the threats to Georgia's election system, (ECF No. 239 ¶¶ 20-22), explaining the scale and sophistication of Russia's attempts to interfere in the 2016 election. (ECF No. 239 ¶ 21.) Dr. Halderman noted that the Mueller Report found that Georgia was among the states targeted by Russia. (ECF No. 239 ¶ 21.) Finally, Dr. Halderman highlighted other nation states with similarly advanced cyberwarfare capabilities, including China, Iran, and North Korea. (ECF No. 239 ¶ 21.)

Rather than "simply list[ing] possibilities, with no explanation of how likely it is that each scenario actually will occur," as Defendants contend, ECF No. 401 at

[7] Defendants sometimes complain that this case is about the 2018 election but, when attacked, they change course, arguing the 2018 election is moot.

7, Dr. Halderman opined that "Georgia's new technology does not achieve the level of security necessary to withstand an attack by a sophisticated adversary such as a hostile foreign government," (ECF No. 239 ¶ 23). To support this opinion, Dr. Halderman provided examples of potential attacks applicable to the Georgia voting systems, as informed by the threats described in the Mueller Report. (ECF No. 239 ¶ 23.) Dr. Halderman used his background and experience with election security to arrive at his conclusions, while also considering previous successful cyber-attacks such as Stuxnet in Iran. (ECF No. 239 ¶ 26.) *See Noe v. Metro. Gen. Ins. Co.*, No. 1:11-cv-02026-SCJ, 2012 WL 7760143, at *3 (N.D. Ga. Dec. 10, 2012) (explaining the expert "outlines his access to industry resources and other research tools, which he used in formulating his opinion, to show his opinion is reliable"). *Compare Fiveash v. Allstate Ins. Co.*, No. 3:13-cv-18-TCB, 2013 WL 12097615, at *4 (N.D. Ga. Aug. 1, 2013) (limiting testimony of expert whose opinions required a "leap of faith").

Finally, Dr. Halderman explained the vulnerabilities in Georgia's voting equipment including the Dominion components, voter registration components, election poll books, and supply chain. (ECF No. 239, ¶¶ 27-51.) Defendants attempt to discredit the reliability of Dr. Halderman's analysis by stating that he "never quantified any of the many risks described." (ECF No. 401 at 7.) But an

expert opinion need not quantify the risk. *See Crow v. United States*, No. 1:16-cv-3104-SCJ, 2018 WL 8919931, at *9 (N.D. Ga. Sep. 10, 2018) ("[T]here is no requirement under the Federal Rule of Evidence 702 that an expert testifying based on knowledge, training, and experience quantify their opinions into statistics.").

Defendants also state that Dr. Halderman "did not evaluate Georgia's new system on its own merits" (ECF No. 401 at 8.), suggesting that he formed his opinions in this matter "based on his own subjective belief or unjustifiably extrapolated from the information before him," *See Flynn v. FCA US LLC*, No. 15-cv-0855, 2018 WL 2063871, at *11 (S.D. Ill. Jan. 31, 2018). On the contrary, he considered materials obtained from Dominion. After reviewing the manufacturer's technical documents, Dr. Halderman used his knowledge and experience in cybersecurity, along with his research and publications, to evaluate the Dominion system. Dr. Halderman is not simply making a public policy argument for a "hand-marked paper ballot system." (ECF No. 401 at 9.) Rather, Dr. Halderman is describing the tangible vulnerabilities presented by BMDs.

Defendants attempt to support their arguments against Dr. Halderman by referencing two distinguishable, politically charged cases from the United States District Court for Eastern District of Pennsylvania in which Dr. Halderman served as an expert. (ECF No. 401 at 10.) *See Stein v. Boockvar*, No. 16-6287, 2020 WL

2063470 (E.D. Pa. Apr. 29, 2020); *Stein v. Cortés*, 223 F. Supp. 3d 423 (E.D. Pa. 2016). Their effort is misplaced. While it is correct that the judge in the *Stein* cases disagreed with Dr. Halderman, his is a singular view of Dr. Halderman's value predicated on unique circumstances. *See Boockvar*, 2020 WL 2063470, at *2-3 (considering the plaintiff's request to decertify Pennsylvania's voting machines because they allegedly did not comply with a settlement agreement); *Cortés*, 223 F. Supp. 3d at 426, 441 (considering whether a recount was required after the 2016 presidential election where Dr. Halderman had access to public materials only).

More relevant for evaluating reliability, all of the following entities have relied on Dr. Halderman's testimony on the security of voting machines: the Senate Intelligence Committee; the United States House Appropriations Subcommittee on Financial Service and General Government (the "House Subcommittee"); and the United States District Court for the Northern District of Georgia. Indeed, the Senate Intelligence Committee cites Dr. Halderman's opinions on Russian interference, and the report specifically references his opinions related to vulnerabilities in the national voting system. *See* Senate Report at 40-42. And Dr. Halderman presented these opinions on voting equipment and election management systems to the House Subcommittee.

In 2018 and 2019, relying on Dr. Halderman's testimony, this Court (Totenberg, J.) decided a case involving the "heightened critical cybersecurity issues" related to voting machines in Georgia. *Curling v. Kemp*, 334 F. Supp. 3d 1303, 1307 (N.D. Ga. 2018); *accord Curling v. Raffensperger*, 397 F. Supp. 3d 1334, 1412 (N.D. Ga. 2019). Dr. Halderman was a central expert witness in the *Curling* cases, where he testified about cybersecurity vulnerabilities in Georgia's voting machines. *Curling v. Kemp*, 334 F. Supp. 3d at 1308-09; *Curling v. Raffensperger*, 397 F. Supp. 3d at 1367, 1377 & n.63. During a 2018 hearing, Dr. Halderman demonstrated "how malware could be introduced into a DRE machine via a memory card and actually change an elector's vote without anyone knowing." *Curling v. Kemp*, 334 F. Supp. 3d at 1323. Not only did the Court credit his testimony, but the also Court explained that the "evidence and testimony presented conforms with the patterns of heightened cybersecurity breach and data manipulation attacks now regularly appearing in civil financial cases as well as criminal cases." *Id*. at 1324.

Ultimately, when ordering Georgia to discontinue its use of the insecure paperless voting machines Defendants staunchly defended, the Court relied extensively on Dr. Halderman's testimony. *Curling v. Raffensperger*, 397 F. Supp. 3d at 1412. Defendants claim Dr. Halderman's opinions are not reliable because

"[h]e simply decided, as a policy matter, that the only acceptable system is hand-marked paper ballots . . . ." (ECF No. 401 at 8.) But, as the Court explained, he is not alone in advancing that view: "[T]he U.S. Senate Select Committee on Intelligence concluded that 'paper ballots and optical scanners are the least vulnerable to cyberattack." *Curling v. Raffensperger*, 397 F. Supp. 3d at 1367 (quoting the Senate Report at 59).

Defendants' assertions that Dr. Halderman's opinions are not reliable because he "adopted a preferred end result and reasoned backward" are wrong. (ECF No. 401 at 8.) Dr. Halderman's opinions regarding cybersecurity vulnerabilities are reliable and supported by his review of documentation and extensive experience. In any event, Defendants' criticisms go only to the weight of the evidence if they can prove them, not its admissibility. *Rosenfeld v. Oceania Cruises, Inc.*, 654 F.3d 1190, 1193 (11th Cir. 2011) ("[I]n most cases, objections to the inadequacies of a study are more appropriately considered an objection going to weight of the evidence rather than its admissibility." (internal quotation marks and citation omitted)).

Dr. Halderman's opinions and analysis are reliable. Before forming his opinions, Dr. Halderman reviewed Georgia's current system; Dr. Halderman also considered critical cyber threats such as those highlighted in the Mueller Report;

and after applying the relevant cyberattacks to the Dominion design and architecture, Dr. Halderman provided opinions about the vulnerabilities in Georgia's current system. As with the opinions he provided for the United States Senate, the House, and the Court in *Curling*, Dr. Halderman used his background and experience to provide a reliable opinion specific to the facts in this case.

C. Dr. Halderman's testimony is relevant and will assist the trier of fact.

Dr. Halderman's "technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue." *See* Fed. R. Evid. 702. "By this requirement, expert testimony is admissible if it concerns matters that are beyond the understanding of the average lay person." *United States v. Frazier*, 387 F.3d 1244, 1262 (11th Cir. 2004) (citing *United States v. Rouco*, 765 F.2d 983, 995 (11th Cir. 1985)). "With respect to the admissibility of an expert's opinion, the term helpfulness is broad and liberally construed." *Flynn*, 2018 WL 2063871, at *3.

Defendants do not dispute that Dr. Halderman's testimony regarding the cybersecurity of the state's electronic voting machines "concerns matters that are beyond the understanding of the average lay person." *See Frazier*, 387 F.3d at 1262. Courts routinely permit testimony from cybersecurity experts, acknowledging that such testimony assists the trier of fact. *See, e.g.*, *Quality Plus*

Servs., Inc. v. Nat'l Union Fire Ins. Co., No. 3:18cv454, 2020 WL 239598, at *11-16, 19 (E.D. Va. Jan. 15, 2020) (denying motion *in limine* and allowing cybersecurity expert to testify); *Flynn*, 2018 WL 2063871, at *7 (denying motion to strike or bar testimony from cybersecurity expert). Instead, Defendants argue that Dr. Halderman's testimony would not assist the trier of fact because it is not relevant and "does not relate to any issue in the case." (ECF No. 401 at 12 (quoting *Kilgore v. Reckitt Benckiser, Inc.*, 917 F. Supp. 2d 1288, 1292 (N.D. Ga. 2013) (denying motion to exclude testimony)).) Defendants are incorrect.

"Expert testimony is considered relevant when 'it logically advances a material aspect of the proposing party's case.'" *Noe v. Metro. Gen. Ins. Co.*, No. 1:11-cv-02026-SCJ, 2012 WL 7760143, at *2 (N.D. Ga. Dec. 10, 2012) (quoting *Allison v. McGhan Med. Corp.*, 184 F.3d 1300, 1312 (11th Cir. 1999)). The Secretary of State's embrace and impassioned defense of machines that can be hacked impugns the integrity of the election process. These vulnerabilities in the voting system heighten voters' concerns. Convincing voters of color that their vote will not count is one of Defendants' many voter suppression tactics. Plaintiffs challenge Defendants' use of voting technology that lacks adequate data security and is vulnerable to hacking, (*see* ECF No. 41 ¶¶ 94-101), including the voter registration database and voting machines that Georgia used in the June 2020

primary election. When so ordered by this Court, Defendants replaced hackable DRE voting machines but chose vulnerable BMDs and continue to use an insecure voter registration system. As Georgia's recent primary election demonstrated, Plaintiffs' prayer for relief—that Defendants ensure each county has and deploys to each polling place for any election day an adequate and reasonable number of functioning and secure voting machines—has yet to be fulfilled. (*See* ECF No. 41 at 91 (Prayer for Relief ¶ 11(e)).)

Insecure voting technology systematically disenfranchises voters of color. The Secretary of State loudly proclaimed that the system was safe when this Court was so concerned that it would have required the use of paper ballots had there been time before the 2020 election. *Curling v. Raffensperger*, 397 F. Supp. 3d at 1405. The insecurity of the voting system was widely publicized in the months before the election. Mark Niesse, *Hackers say they took over vote scanners like those coming to Georgia*, Oct. 4, 2019, https://www.ajc.com/news/state--regional-govt--politics/hackers-say-they-took-over-vote-scanners-like-those-coming-georgia/0vZH2fNqGhN27JBpDK0ZfJ/. To reassure voters of the safety of the systems, if Defendants believed that, they might have said "we are concerned, and we will investigate and resolve the issues raised." Instead, the Sunday before the 2018 election, the Secretary of State who had resigned the prior week announced

falsely that the Democratic Party of Georgia had tried to hack the system. He also falsely announced an FBI investigation.[8] It would be difficult to believe Governor Kemp's announcements were intended to assure the electorate that the DRE machines were secure.

Dr. Halderman testified the problems he identified in his report "certainly could have a racial effect, especially if an attacker seeking to so[w] discord or alter the outcome of an election targeted specific candidates or racial groups for that effect." (ECF No. 401-1 at 14:4-8.) Dr. Halderman is not alone in his view. When asked if Plaintiff Ebenezer would "stop diverting funds" to address these tactics if Plaintiffs receive the relief sought, Reverend Raphael Warnock testified that "[w]hether or not there would be other barriers, when I look at the long history of voter suppression, very long history, since the end of Reconstruction, the efforts to constrict the participation of people of color particularly have proven to be incredibly creative and agile." (Ex. 5, (Warnock Dep. 188:8 – 189:14).) Thus, the effect of Defendants' defense of current voting systems remains "a material aspect of [Plaintiffs'] case.'" *Noe*, 2012 WL 7760143, at *2.

[8] The GBI investigated an individual, not the Democratic Party, and found no basis for the SOS's claim.

Dr. Halderman's opinions that the 2018 and current voting systems are vulnerable are relevant to this method of voter suppression. Defendants should prefer a safe system. That they do not has the expected effect of discouraging citizens from voting. Dr. Halderman's testimony "logically advances," *Noe*, 2012 WL 7760143, at *2, Plaintiffs' allegations that "Defendants use election technology that is vulnerable to hacking and manipulation." (ECF No. 41 at 41.)

CONCLUSION

Defendants' motion in limine to exclude Dr. Halderman's testimony should be denied.

CERTIFICATE OF COUNSEL REGARDING FONT SIZE

I hereby certify that the foregoing has been prepared with a font size and point selection (Times New Roman, 14 pt.) which is approved by the Court pursuant to Local Rules 5.1(C) and 7.1(D).

Respectfully submitted, this, the 27th day of July, 2020.

/s/ Allegra J. Lawrence
Allegra J. Lawrence (GA Bar No. 439797)
Leslie J. Bryan (GA Bar No. 091175)
Maia Cogen (GA Bar No. 832438)
Suzanne Smith Williams (GA Bar No. 526105)
LAWRENCE & BUNDY LLC

1180 West Peachtree Street
Suite 1650
Atlanta, GA 30309
Telephone: (404) 400-3350
Fax: (404) 609-2504
allegra.lawrence-hardy@lawrencebundy.com
leslie.bryan@lawrencebundy.com
maia.cogen@lawrencebundy.com
suzanne.williams@lawrencebundy.com

Thomas R. Bundy (Admitted *pro hac vice*)
LAWRENCE & BUNDY LLC
8115 Maple Lawn Boulevard
Suite 350
Fulton, MD 20789
Telephone: (240) 786-4998
Fax: (240) 786-4501
thomas.bundy@lawrencebundy.com

Dara Lindenbaum (Admitted *pro hac vice*)
SANDLER REIFF LAMB ROSENSTEIN & BIRKENSTOCK, P.C.
1090 Vermont Avenue, NW
Suite 750
Washington, DC 20005
Telephone: (202) 479-1111
Fax: 202-479-1115
lindenbaum@sandlerreiff.com

Elizabeth Tanis (GA Bar No. 697415)
John Chandler (GA Bar No. 120600)
957 Springdale Road, NE
Atlanta, GA 30306
Telephone: (404) 771-2275
beth.tanis@gmail.com
jachandler@gmail.com

Kurt G. Kastorf (GA Bar No. 315315)
KASTORF LAW, LLC
1387 Iverson St, Suite 100
Atlanta, GA 30307
Telephone: (404) 900-0330
kurt@kastorflaw.com

Matthew G. Kaiser (Admitted *pro hac vice*)
Sarah R. Fink (Admitted *pro hac vice*)
Scott S. Bernstein (Admitted *pro hac vice*)
Norman G. Anderson (Admitted *pro hac vice*)
KAISERDILLON PLLC
1099 Fourteenth Street, NW
Eighth Floor West
Washington, DC 20005
Telephone: (202) 640-2850
Fax: (202) 280-1034
mkaiser@kaiserdillon.com
sfink@kaiserdillon.com
sbernstein@kaiserdillon.com
nanderson@kaiserdillion.com

Andrew D. Herman (Admitted *pro hac vice*)
Nina C. Gupta (Admitted *pro hac vice*)
MILLER & CHEVALIER CHARTERED
900 Sixteenth Street, NW
Washington, DC 20006
Telephone: (202) 626-5800
Fax: (202) 626-5801
aherman@milchev.com
ngupta@milchev.com

Kali Bracey (Admitted *pro hac vice*)
Ishan Bhabha (Admitted *pro hac vice*)
JENNER & BLOCK LLP
1099 New York Avenue, NW
Suite 900
Washington, DC 20001
Telephone: (202) 639-6000
Fax: (202) 639-6066
kbracey@jenner.com
ibhabha@jenner.com

Jeremy M. Creelan (Admitted *pro hac vice*)
Elizabeth A. Edmondson (Admitted *pro hac vice*)
JENNER & BLOCK LLP
919 Third Avenue
New York, New York 10022
Telephone: (212) 891-1600
Fax: (212) 891-1699
jcreelan@jenner.com
jershow@jenner.com
eedmondson@jenner.com

Von A. DuBose
DUBOSE MILLER LLC
75 14th Street N.E., Suite 2110
Atlanta, GA 30309
Telephone: (404) 720-8111
Fax: (404) 921-9557
dubose@dubosemiller.com

Johnathan Diaz (Admitted *pro hac vice*)
Paul M. Smith (Admitted *pro hac vice*)
CAMPAIGN LEGAL CENTER
1101 14th St. NW Suite 400
Washington, DC 20005
Telephone: (202)736-2200
psmith@campaignlegal.org
jdiaz@campaignlegal.org

Counsel for Fair Fight Action, Inc.; Care in Action, Inc.; Ebenezer Baptist Church of Atlanta, Georgia, Inc.; Baconton Missionary Baptist Church, Inc.; Virginia-Highland Church, Inc.; and The Sixth Episcopal District, Inc..

CERTIFICATE OF SERVICE

I hereby certify that I filed the foregoing **PLAINTIFFS' RESPONSE IN OPPOSITION TO DEFENDANTS' MOTION TO EXCLUDE THE EXPERT TESTIMONY OF J. ALEX HALDERMAN** using the Court's ECF System, which will send copies to all counsel of record.

This, the 27th day of July, 2020.

/s/ Allegra J. Lawrence
Allegra J. Lawrence